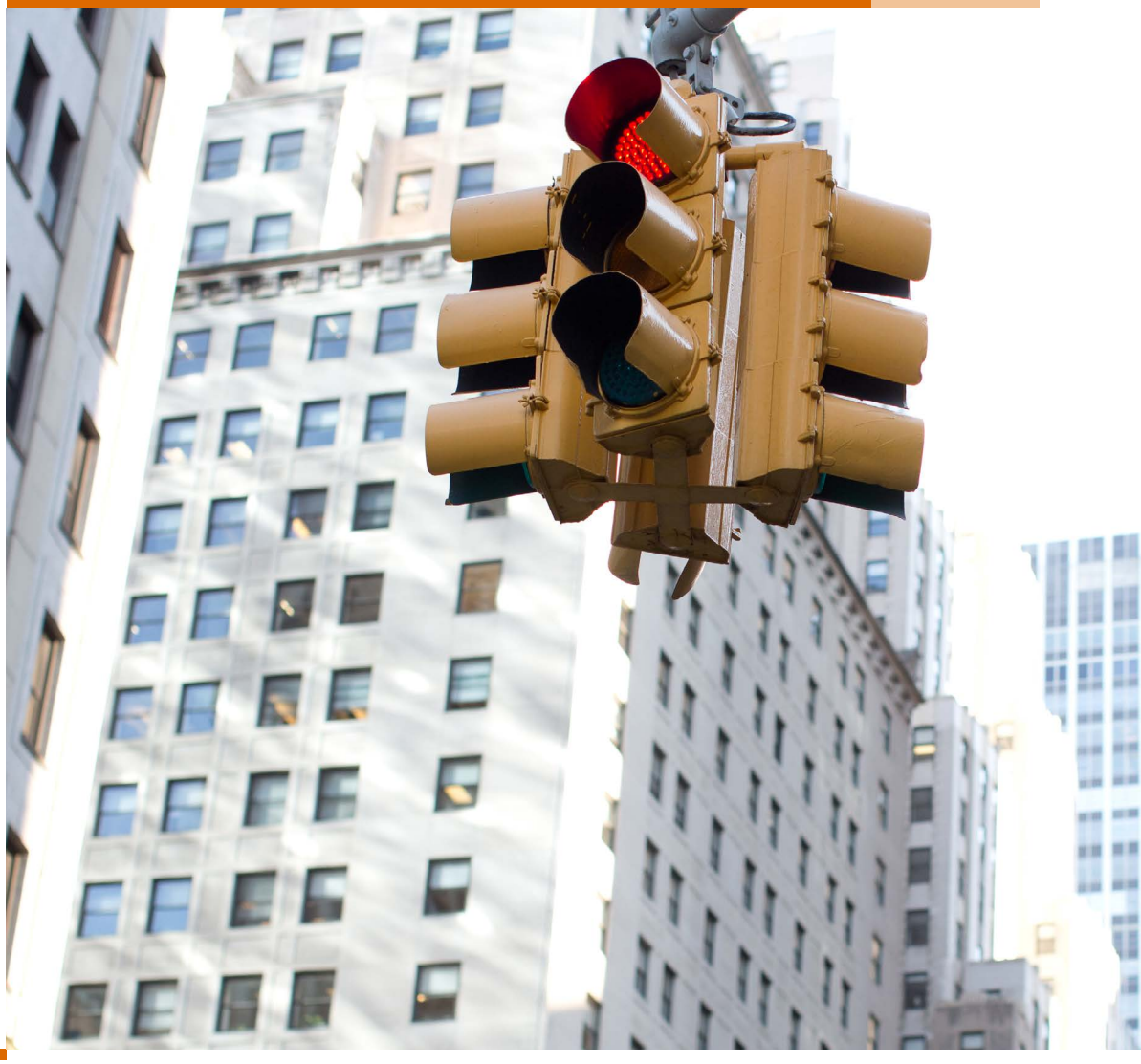
www.pwc.com/cybersecurity

US cybersecurity: Progress stalled

Key findings from the 2015 US State of Cybercrime Survey

July 2015



pwc

About the 2015 US State of Cybercrime Survey

The 2015 US State of Cybercrime Survey was co-sponsored by PwC, *CSO,* the CERT® Division of the Software Engineering Institute at Carnegie Mellon University, and the United States Secret Service.

Cybersecurity leaders from these organizations worked together to evaluate survey responses from more than 500 executives of US businesses, law enforcement services, and government agencies. We evaluated trends in the frequency and impact of cybercrime incidents, cybersecurity threats, information security spending, and the risks of third-party business partners in private and public organizations. We also assessed how businesses are adapting to evolving expectations of the information security function and the Board of Directors.

In addition to analysis of the survey results, this report also draws on previous PwC research that includes PwC's 18th Annual Global CEO Survey, The Global State of Information Security® Survey 2015, and the 2015 Digital IQ Survey. We leveraged these surveys to provide a more thorough and balanced look into the current state of cybersecurity and cyberthreats.

It's been a watershed year for cybercrime

Cybercrime continues to make headlines—and cause headaches among business executives.

76%

said they are more concerned about cyberthreats this year.

Cybersecurity incidents are not only increasing in number, they are also becoming progressively destructive and target a broadening array of information and attack vectors. It's clear that adversaries continue to advance their threats, techniques, and targets. They are investing in technologies, sharing intelligence, and training their crews to attack with purpose and competence.

It's no wonder, then, that we found rising concern among the 500 US executives, security experts, and others from the public and private sectors who participated in the 2015 US State of Cybercrime Survey. In fact, 76% of respondents said they are more concerned about cybersecurity threats this year than in the previous 12 months, up from 59% the year before. We have noticed a similar increase in apprehension in other research. In PwC's 18th Annual Global CEO Survey 2015, for example, 87% of US chief executives said they were worried that cyberthreats could impact growth prospects, up from 69% the year before.[1]

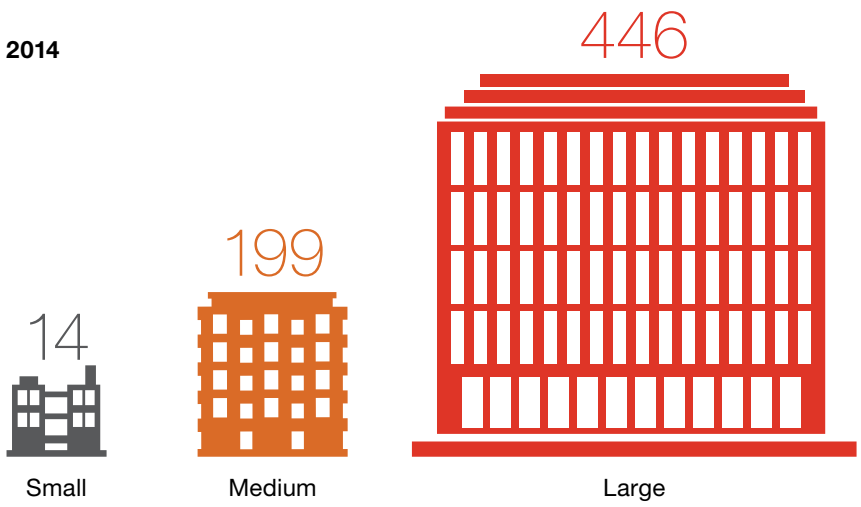
Heightened awareness and concern are well-warranted: A record 79% of survey respondents said they detected a security incident in the past 12 months. Many incidents go undetected, however, so the real tally is probably much higher.

We found a significant correlation between company size and the ability to detect cybersecurity incidents. As a general rule, larger organizations tend to identify more incidents year over year. In fact, respondents from large businesses detected 31 times more incidents than small companies. It's a pattern we have observed in previous research. In The Global State of Information Security® Survey 2015, large organizations detected 28% more incidents in 2014 compared with the year before, while small companies detected 5% fewer incidents during the same time period.[2]

These findings make sense, given that bigger organizations tend to have mature security technologies, processes, and resources that enable them to detect more incidents.

Not surprisingly, the most-frequently cited types of compromise are typically crimes committed by external threat actors, those who are not employees or third-party partners with trusted access to networks and data. Particularly worrisome are phishing campaigns, which are comparatively easy to initiate and can rapidly spread across an organization, targeting top executives as well as employees and managers. Almost one-third (31%) of respondents said they had been hit by a phishing attack in 2014, making it one of the most frequent types of incidents.

Detected incidents by company size*



** Size by number of employees Small: Fewer than 1,000; Medium: 1,000 to 9,999; Large: 10,000 or more*

1 PwC, 18th Annual Global CEO Survey, January 2015

2 PwC, *CSO, CIO* magazine, The Global State of Information Security® Survey 2015, September 2014

The lines separating the intents of nation-states, hacktivists, and organized crime are beginning to blur.

Cyberattacks are becoming more destructive

Globally, a record 1 billion data records were compromised in 2014, according to a report by security firm Gemalto.[3] Many of those security incidents were very widely reported: The year 2014 saw the term "data breach" become part of the broader public vernacular, with *The New York Times* devoting more than 700 articles related to data breaches, versus fewer than 125 the previous year.[4]

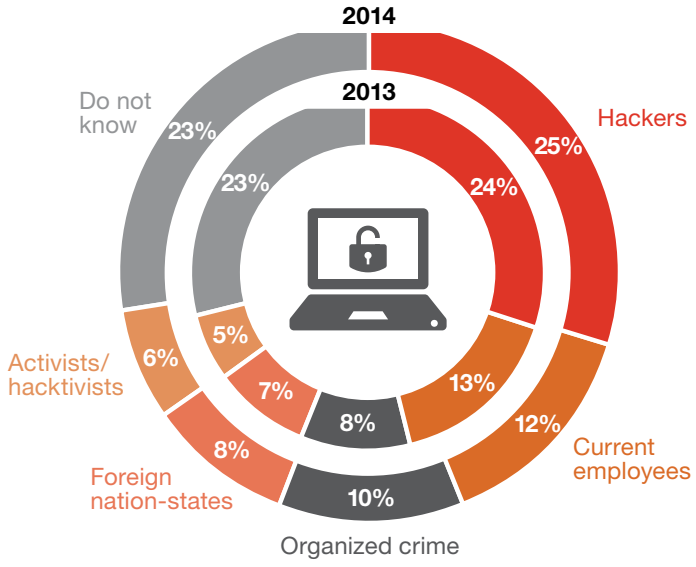
It's not just the number of incidents—detected or not—that's on the rise. Attacks are also becoming increasingly public and prominent.

In the past, public knowledge of cybercrime was typically limited to only those incidents requiring disclosure. That, as it turns out, was merely the tip of the iceberg. The huge mass of risks (and attacks) once lurking below the surface are now splashed across websites, social media, and newspapers on a daily basis. In part, that's because behavior of threat actors has become increasingly egregious, and their attacks can be progressively more destructive.

The high-profile assault on a global entertainment company late last year demonstrated that threat actors' motives and means are varied, and that lines separating the intents of nation-states, hacktivists, organized crime, and individuals with malicious intent are beginning to blur. The perpetrator of the hack, thought to be a nation-state acting on political motivations, released personal data and damaging employee communications, as well as sensitive corporate documents and payroll information. The attack also disrupted the company's email and telephone systems, and introduced a new level of malice that included a threat of physical violence to individuals.

As motives and means continue to evolve, so do the methods of attack. Distributed denial of service (DDoS) attacks are becoming increasingly potent and are one of the most frequent types of cybersecurity incidents, cited by 18% of survey respondents this year. DDoS assaults most often result in damage to reputation, but they also can put businesses at risk by disrupting e-commerce and other business processes.

Greatest cyberthreats to organizations



3 Gemalto, Gemalto Releases Findings of 2014 Breach Level Index, February 12, 2015

4 Verizon, 2015 Data Breach Investigations Report, April 15, 2015

The retail and consumer products industry, after two years of high-profile attacks, significantly increased information security spending.

Ransomware, a comparatively new type of cybercrime, is becoming more sophisticated and commonplace. The FBI recently warned that this type of attack, in which adversaries take control of a company's data until it pays a ransom, is on the rise.[5] In 2014, 13% of Cybercrime Survey respondents said they had been a victim of ransomware. We expect that reports of ransomware will continue to mount.

Some categories of cybercrime have been around for decades, but rarely spark the interest of the media. Take wire fraud. While not widely reported, this type of cybercrime is becoming more prominent and costly. The FBI and the Internet Crime Complaint Center recently said that global wire fraud cost businesses $215 million during a 14-month period, with US companies representing 84% of those financial losses.[6] Our survey shows that 21% of law enforcement respondents cited wire fraud as among the top five areas that consume their caseload time. It's a crime that frequently begins with phishing campaigns that often target top executives.

Large companies and retailers boost security spending

On a more positive note, the recent rash of security incidents may be convincing companies to step up their investments in cybersecurity.

While this survey did not measure the average security budgets of respondents, in The Global State of Information Security® Survey 2015 we found that US information security budgets have grown at almost double the rate of IT budgets over the last two years.[7]

The Cybercrime Survey indicated that industries that have been impacted by high-profile cyberattacks were more likely to significantly boost information security investments. In fact, 38% of retail and consumer companies, which have been frequent targets of attack in the past two years, increased their security spending by 20% or more over the year before—higher by far than any other industry. By contrast, only 17% of banking and finance and 15% of healthcare respondents reported 20% increases in security budgets.

The appropriate level of cybersecurity investment will vary by industries and their threat environments, of course. A spending increase of 20% or more may be unnecessary for banking and finance organizations, which typically spend more on security than businesses in other sectors. Healthcare organizations, by comparison, tend to spend less on cybersecurity yet are being hit with new types of attacks across expanded vectors. The PwC Health Research Institute predicts that recent data breaches will prompt health companies to take extra steps to protect sensitive personal information and increase investments in information security.[8] While the Cybercrime Survey did not ask respondents about information security budgets for 2015, The Global State of Information Security® Survey found that 51% of healthcare payers and providers plan to boost security spending in 2015.[9]

The Cybercrime Survey determined that large businesses were more likely to substantially increase information security spending. In fact, 20% of companies with more than 10,000 employees said they raised security investments by 20% or more in 2014, while 12% of small companies did so.

This explains, in part, why large companies typically have more mature security practices: They have consistently invested more over the years.

No matter the size, as companies boost their security budgets, executives will likely place a greater emphasis on the return on investment in cybersecurity. After all, they will want to make sure that the increased spending results in measurable improvements in the company's security posture.

5 Federal Bureau of Investigation, Ransomware on the Rise, January 20, 2015

6 eWeek, Spam Campaign Business E-mail Compromise Pilfers $215 Million, January 23, 2015

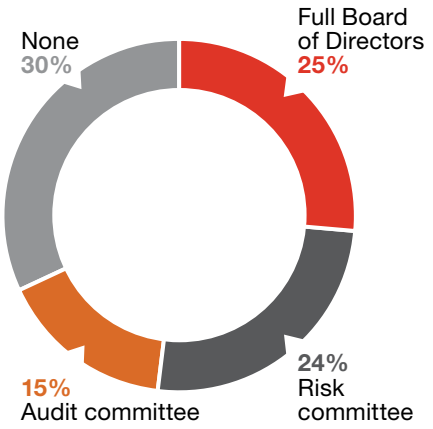
7 PwC, *CSO, CIO* magazine, The Global State of Information Security® Survey 2015, September 2014

8 PwC Health Research Institute, Medical Cost Trend: Behind the Numbers 2016, June 2015

9 PwC, *CSO, CIO* magazine, The Global State of Information Security® Survey 2015, September 2014

Almost half of Boards still view cybersecurity as an IT matter, rather than an enterprise-wide risk issue.

Board engagement in cyber-risks



Boards are concerned, but not always engaged

Another result of the barrage of breaches over the past year is that many Boards of Directors now take a very active interest in cybersecurity. They want to know about current and evolving risks, as well as the organization's security preparedness and response plans. The question is how often security leaders provide cyber-risk briefings to their Boards.

Our research shows that one in four (26%) respondents said their Chief Information Security Officer (CISO) or Chief Security Officer (CSO) makes a security presentation to the Board only once a year, while 30% of respondents said their senior security executive makes quarterly security presentations. But 28% of respondents said their security leaders make no presentations at all.

As with other cybersecurity best practices, CISOs and CSOs from large companies are more likely to make quarterly Board presentations and small organizations are least likely to do so. In fact, one-third (33%) of respondents from small companies said their security leaders never advise the Board on security risks, compared with 18% of large companies.

While there is no universal approach to Board participation in oversight of cyber-risks, as a general guideline the National Association of Corporate Directors (NACD) recommends that risk oversight be a function of the full Board. The critical link between strategy and risks points to the need for the full Board—and not just one committee—to have responsibility for cybersecurity risk, according to the NACD.[10] So it was a bit worrisome to find that 30% of respondents said no Board committees or members are engaged in cyber-risks. At the other end of the spectrum, only 25% of respondents said their full Board is involved in cyber-risks.

It seems curious that just 15% of respondents said the audit committee is engaged in cyber-risks. In the past several years, we have seen many companies add a raft of internal insight issues—including cybersecurity—to the audit committee's agenda. One explanation for the comparatively weak engagement of the audit committee may be that companies are shifting cybersecurity oversight responsibilities to the entire Board or special risk committees.

10 National Association of Corporate Directors, Cyber-Risk Oversight: Directors Handbook Series, 2014

Security executives should not wait for the Board to ask questions about cyber-risks and cybersecurity preparedness.

These statistics are alarming when viewed through a post-breach lens. The lack of substantive consideration of operational cyber-risks by the Board may lead regulators and plaintiff's counsel to conclude the operational risk lacked preventive and detective controls that management is responsible for implementing and the Board is responsible for monitoring.

It's also essential that Boards treat cybersecurity as an overarching corporate risk issue rather than simply an IT risk. Many have yet to adopt this approach, however. Almost half (49%) of Boards view cybersecurity as an IT risk, while 42% see cybersecurity through the lens of corporate governance.

Organizations that treat cybersecurity as a matter of enterprise-wide risk should be able to demonstrate to external stakeholders that they understand and appropriately manage cybersecurity activities and related obligations, as well as the intent to be a good corporate citizen. This level of engagement and awareness often requires a carefully designed oversight program based on corporate governance methodologies and corporate standards that have succeeded in the past. An oversight program can help companies streamline Board reporting, integrate multi-department activities required to mitigate operational cyber-risks, and demonstrate that reasonable security protocols and procedures are in place.

In an effort to better understand enterprise risk, some forward-looking organizations are moving toward a formalized quantitative estimate of cyber-risks and exposures, an approach typically referred to as cybersecurity value at risk. This quantitative estimate is developed within a conceptual framework consistent with traditional financial services value at risk methods. It can help CEOs, CROs, and Boards better understand what digital assets are at risk, how to project potential losses, and how to abate risks using alternative security models, investments, and cybersecurity insurance.

One thing is clear: Security executives should not wait for the Board to ask questions about cyber-risks and cybersecurity preparedness. CISOs and CSOs should proactively update the Board on cybersecurity risks on a semiannual basis—at the very least.

7 reasons why cybersecurity is a Board oversight issue

Cyberthreats are among the most significant business risks facing organizations today—and Boards are now held accountable. As a result, directors must view cybersecurity as an enterprise-wide risk issue that should be addressed from strategic, cross-functional, and economic perspectives. Following are seven reasons why Boards should be asking serious questions about cyberthreats and their organization's cybersecurity capabilities:

1. The impact of cybersecurity is systemic. Incidents can impact an organization's global operations even when a risk point is thousands of miles away.
2. The financial impact can be significant and can include costly class-action lawsuits, which may reflect on Boards' fiduciary responsibility to preserve corporate financial value.
3. As regulations evolve, compliance is becoming more challenging and increasingly costly. The European Union's Data Protection Directive, for instance, includes a proposal for fines of up to 5% of a company's global revenue.[11] This also lays the foundation for civil litigation.
4. The Internet of Things has brought new threats, including compromise of industrial controls and smart building systems that can cause extreme risks and tremendous physical damage.
5. Cybersecurity insurance should be considered as a regulatory hedge against cyber-risks. A risk committee should ask questions regarding coverage for directors' and officers' liability, commercial general liability, prior acts, and property and casualty insurance.
6. Adversaries such as nation-states and organized crime are working together to attack organizations for objectives like economic sabotage, theft of trade secrets, money laundering, terrorism, and military and intelligence operations.
7. Cyberattacks can result in substantial financial losses and damage brand reputation by disrupting an organization's strategic objectives, such as a planned merger or acquisition, the launch of a new product, or a business deal with a potential customer.

11 European Commission, Stronger data protection rules for Europe, June 15, 2015

New ISAOs will be more flexible, enabling businesses to share information across industries as well as by issues, geographies, and specific threats.

Information sharing is front and center

To say that information sharing is having a moment would be an understatement. And President Barack Obama's February 2015 executive order calling for the creation of new Information Sharing and Analysis Organizations (ISAOs) is clearly fueling the discussion.

Sharing reliable, actionable, and timely intelligence advances situational awareness of threats, defense agility, informed decision-making, and rapid notification to affected customers and businesses as well as regulatory bodies. It's also a relatively inexpensive way to gain a fuller picture of threats facing an organization.

Despite the benefits, we found an underwhelming level of participation in industry-specific Information Sharing and Analysis Centers (ISACs): Only 25% of respondents said they were involved in ISACs in 2014, virtually the same as the year before. Industries most likely to participate are electric power, water, banking and finance, and government agencies.

Many industry observers anticipate that the president's executive order will boost participation in information-sharing initiatives. Unlike today's industry-specific ISACs, membership in ISAOs will be more flexible, enabling businesses and public-sector agencies to share information specific to individual industries as well as intelligence related to geographies, issues, events, or threats.

ISAOs may also enable organizations to share information across industries. For example, significant challenges often do not differ by sector (such as financial services or pharmaceuticals) but rather by an entity's size or constituency. A big Wall Street bank might have more in common with a large pharmaceutical company than it does with a regional bank. Indeed, middle-market participants often have different challenges than larger businesses.

ISAOs might resolve these issues, but many foundational objectives must first be addressed. A successful information-sharing model will require a clear mission and focus, should be operated by rules determined (and strictly enforced) by its members, must clearly demonstrate value to its membership, and generate and sustain trust.

A key roadblock to information sharing is a lack of a unified framework, platform, and data standards. Threat intelligence and response tactics should be distributed in real time—which will be impossible to achieve without an integrated and automated infrastructure. To this end, the Department of Homeland Security and others are working to promote specific, standardized message and communication formats such as TAXII, STIX, and CybOX. Clear data on their adoption rates is not yet available, however, nor do we know if they represent the best possible formats.

One thing we do know is that speed is of the essence. Based on attacks observed by cyberthreat firm RiskAnalytics during 2014, 75% of attacks spread from victim 0 to victim 1 within one day (24 hours). Over 40% hit the second organization in less than an hour.[12]

Finally, a successful information-sharing model will need to provide clear guidelines on the privacy of consumer data, as well as a resolution to the thorny public-private conflict on the use of encryption by technology companies. US lawmakers are currently considering information-sharing legislation that, if enacted, may eliminate some of these roadblocks.

12 Verizon, 2015 Data Breach Investigations Report, April 15, 2015

A lopsided investment in technology

Although cybersecurity budgets are on the rise, for better or worse, surging anxiety about cybercrime has led to a greater reliance on technology solutions to fend off digital adversaries and manage risks.

Consider that 75% of US chief executives responding to PwC's 18th Annual Global CEO Survey ranked cybersecurity solutions as "very important" to the company's business strategy.[13] We found a similar enthusiasm for technology in PwC's 2015 Digital IQ Survey: 69% of respondents said they are investing in cybersecurity technologies, more than any other spending category.[14]

So it was not surprising to find that respondents to the US Cybercrime Survey are similarly bullish on technology. Almost half (47%) said adding new technologies is a spending priority, higher than all other initiatives. Notably, only 15% cited redesigning processes as a priority and 33% prioritized adding new skills and capabilities.

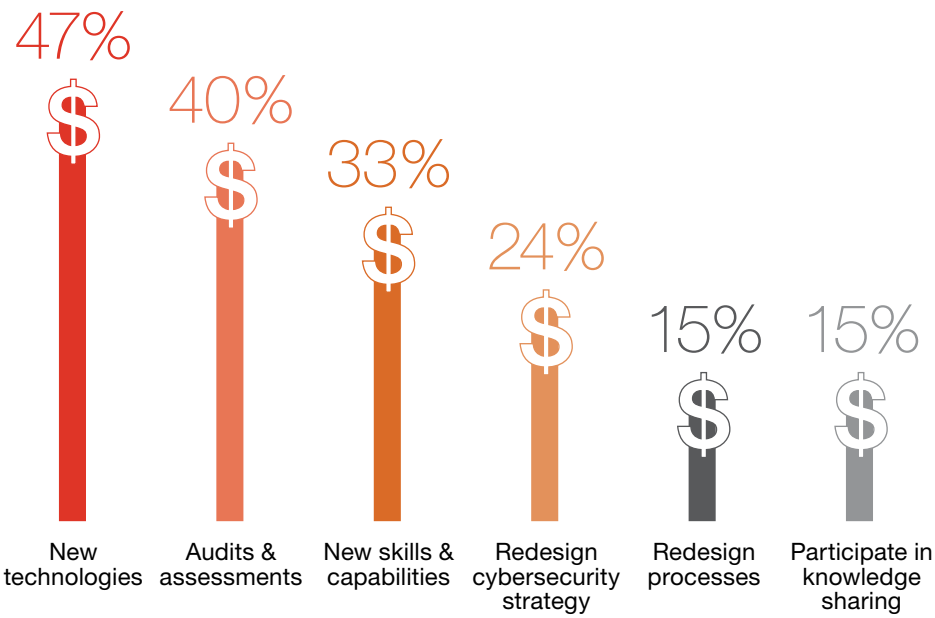
When we asked whether organizations have the expertise to address cyber-risks associated with implementation of new technologies, only 26% said they have capable personnel on staff. Most rely on a combination of internal and external expertise to address cyber-risks of new solutions.

Companies that implement new technologies without updating processes and providing employee training will very likely not realize the full value of their spending. To be truly effective, a cybersecurity program must carefully balance technology capabilities with redesigned processes and staff training skills.

Employee training and awareness continues to be a critical—and often neglected—component of cybersecurity. Only half (50%) of survey respondents said they conduct periodic security awareness and training programs, and the same number offer security training for new employees.

In addition to a thorough employee security awareness program, it will also be critical to have regularly tested and updated incident-response and crisis-management playbooks in place. These plans should include frequent tabletop exercises for security and business stakeholders, as well as ongoing training for employees and executive leaders. In today's cybercrime environment, the issue is not whether a business will be compromised, but rather how successful an attack will be; organizations that are well-prepared will have a better ability to limit the impact. Preparedness will also enable security executives to convey confidence and control to the C-suite and Board.

Cyber-risk spending priorities



13 PwC, 18th Annual Global CEO Survey, January 2015

14 PwC, Three surprising digital bets for 2015, January 2015

Regulators in the financial services industry are leading the charge in focusing on due diligence of third-party suppliers.

Third-party risks are not adequately addressed

The need for due diligence of the security capabilities of third parties has gained prominence in the past year, in part because of high-profile breaches that began with attacks on the systems of business partners.

That's not to say the need to assess the cybersecurity of third parties is new, however. What's different is that regulators are becoming increasingly serious about third-party risk management and expect that organizations will be able to prove due diligence, as well as ongoing supervision and governance.

Regulators in the financial services industry are leading the charge. The Federal Financial Institutions Examination Council (FFIEC) has developed a Cybersecurity Assessment Tool to help institutions identify risks and determine their cybersecurity maturity. Management can use the tool to assess the institution's inherent risk profile based on technologies and connection types, delivery channels, online and mobile products and technology services, organizational characteristics, and external threats.[15]

The New York State Department of Financial Services is focusing on security assessments of third-party providers. In October 2014, the department polled 40 regulated banking organizations for information about due diligence, policies and procedures, safeguards for sensitive data, and protections against loss incurred as a result of third-party information security failures.[16]

This increased regulatory scrutiny is likely to spread to other industries, so it was encouraging to see some advances in the number of respondents who assess risks associated with supply chains and business ecosystems. This year, 62% said they evaluate the security risks of third-party partners and 57% said they do so for contractors, while only 42% of respondents consider supplier risks.

Assessment of business ecosystem risks

15 Federal Financial Institutions Examination Council, Cybersecurity Assessment Tool, June 2015

16 New York State Department of Financial Services, Update on Cyber Security in the Banking Sector: Third Party Service Providers, April 2015

Almost one in five (19%) of C-suite executives said they are not concerned about cybersecurity risks associated with third-party and supply chain partners.

But it's worrisome that almost one in five (19%) CEOs, CFOs, and COOs said they are not at all worried about any kind of supply-chain risk. It may be that many of these executives presume that the IT department is responsible for third-party threats. If so, we've got some potentially troubling news for them: 19% of CIOs themselves were unconcerned about supply-chain risks.

It's clear, then, that due diligence of business partners is far from adequate. If you need further proof, consider that only 16% of respondents said they evaluate third parties' cybersecurity more than once a year—and 23% do not evaluate third parties at all. Similarly, most companies do not have a process for assessing the cybersecurity capabilities of third-party partners before they do business with them, nor do they conduct incident-response planning with external partners.

It is essential that the right to assess a partner's security capabilities is stipulated in contracts. Organizations that do not legally plan for due diligence when executing contracts or preparing for a potential M&A transaction may not be allowed to later perform adequate assessments. Also consider that an increasing proportion of security spending occurs outside of the IT function on services like cloud computing. Contracts executed outside of IT may not allow for due diligence and, in fact, they may not require critical information security and privacy safeguards.

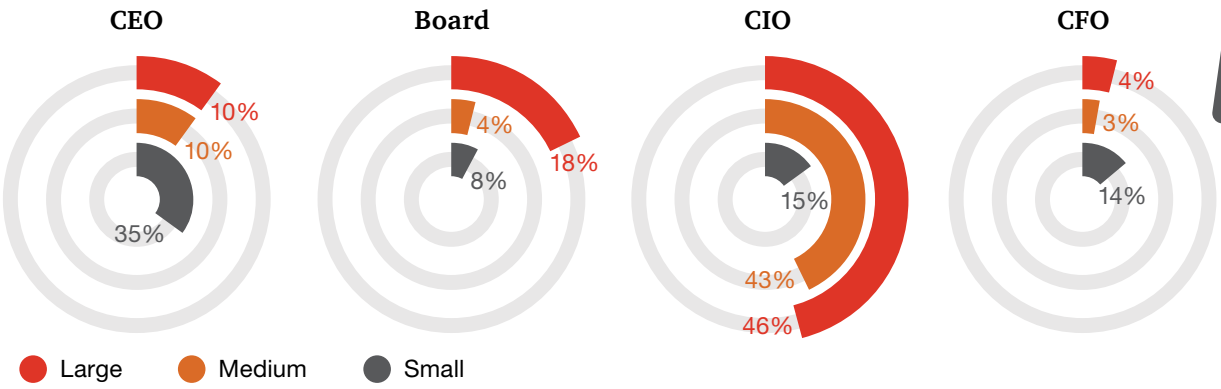
As noted, it will be equally essential that businesses implement and regularly test a response plan for third-party breaches. In the pressure of the moment, incident-response plans may fall apart if they are not well-tested and continually updated.

The strategic role of the CISO

The role and responsibilities of the Chief Information Security Officer continue to evolve as cybercrime becomes a more prominent enterprise-wide risk. This has amplified the debate about how to integrate the security function into the organizational structure and to whom the top security executive should report.

Our survey found that most CISOs and Chief Security Officers report to the CIO, followed by the CEO, CFO, COO, and the Board, in that order. While the organizational structure varies by industry and company size, most sectors follow these patterns, with the CIO being the most likely reporting structure in almost all sectors.

Where the CISO/CSO reports by company size*



** Size by number of employees Small: Fewer than 1,000; Medium: 1,000 to 9,999; Large: 10,000 or more*

In this year's Cybercrime Survey, we found that the top security executive is most likely to report to the CEO in small organizations, while in medium-size companies the CISO or CSO reports to the CIO. Among large companies, the security leader typically reports to the CIO or the Board.

The fact that security leaders most often report to the CIO suggests that organizing the security function under IT is the most effective structure. In reality, this broad generalization does not hold true because the right organizational structure depends on a variety of individual factors, and the role of the CIO differs across companies and industries. In financial services, for example, bank regulators have demanded greater accountability from CISOs and have taken steps to ensure that security leaders do not directly report to the CIO. We have also seen that the role of the CISO is evolving to include both risk as well as security technologies, and that the reporting line is sometimes split between risk officers and general counsel, in addition to dotted-line reports to IT. We expect the role of the CISO to continue to evolve as cybersecurity risks continue to escalate.

No matter the formal organizational structure, the CISO's responsibilities and competencies have irrevocably deepened in the past several years. The role is more senior—and visible—than ever before. The CISO is held accountable for risks, and is expected to deliver a minimum information security posture across the organization.

Today's CISO should be a general manager who has the same level of experience as C-suite officers. He or she should have expertise not only in security but also risk management, corporate governance, and communications. The security leader should have access to key executives to provide insight into business risks and should be able to competently articulate risk-based security issues to the C-suite, Board, and oversight groups like audit, legal, and compliance. Put simply, the information security leader should have the ability to effect change on par with other senior executives.

It's time to take a stance

It's clear that the threats, techniques, and targets of adversaries continue to dynamically—and successfully—evolve. Cybercriminals are investing in technologies, sharing intelligence, and attacking with purpose and persistence.

Businesses must keep up with the capabilities of their adversaries. It's essential to note, however, that keeping pace is not simply a matter of increased cybersecurity spending. Rather, staying abreast of threats may require that organizations redirect limited resources to initiatives that deliver the greatest return. These can include enhanced threat analytics capabilities, prioritizing security of the most critical assets, performing simulations to improve response capabilities across the organization, and stepping up security awareness efforts. Organizations also should be prepared to proactively share information on cybersecurity threats and response tactics. A sustained effort, from the Board down to individual employees, will be needed for many years to come.

We've said it before and we'll say it again: The time for change is now. Organizations must summon the vision, determination, skills, and resources to build a risk-based cybersecurity program that can quickly detect, respond to, and limit fast-moving threats. Those that do not risk becoming tomorrow's front-page news.

Contacts

To have a deeper conversation about cybersecurity, please contact:

David Burg
Principal
david.b.burg@us.pwc.com

Michael Compton
Principal
michael.d.compton@us.pwc.com

Peter Harries
Principal
peter.harries@us.pwc.com

John D. Hunt
Principal
john.d.hunt@us.pwc.com

Mark Lobel
Principal
mark.a.lobel@us.pwc.com

Gary Loveland
Principal
gary.loveland@us.pwc.com

Joseph Nocera
Principal
joseph.nocera@us.pwc.com

Shawn Panson
Partner
shawn.panson@us.pwc.com

Grant Waterfall
Partner
grant.waterfall@us.pwc.com

Contributing authors

Charles Beard
Principal
charles.e.beard@us.pwc.com

Kevin Mickelberg
Director
kevin.j.mickelberg@us.pwc.com

Emily Stapf
Prinicpal
emily.stapf@us.pwc.com

Don Ulsch
Managing Director
don.ulsch@us.pwc.com

www.pwc.com/cybersecurity

© 2015 PricewaterhouseCoopers LLP, a Delaware limited liability partnership. All rights reserved. PwC refers to the US member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. MW-15-2308

PricewaterhouseCoopers has exercised reasonable care in the collecting, processing, and reporting of this information but has not independently verified, validated, or audited the data to verify the accuracy or completeness of the information. PricewaterhouseCoopers gives no express or implied warranties, including but not limited to any warranties of merchantability or fitness for a particular purpose or use and shall not be liable to any entity or person using this document, or have any liability with respect to this document. This report is intended for internal use only by the recipient and should not be provided in writing or otherwise to any other third party without PricewaterhouseCoopers express written consent.